CLAIMS

WHAT IS CLAIMED:

1. A communications system, comprising:

a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal; and

a processing unit adapted to execute a standard mode driver in a standard mode of operation and a privileged mode driver in a privileged mode of operation, wherein the standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer hardware assigned transmission parameters based on the control codes, and the privileged mode driver includes program instructions adapted to independently extract secure control codes from the digital received signal, determine an operational characteristic of the physical layer hardware unit, and signal a security violation in response to the operational characteristic being inconsistent with the secure control codes.

2. The system of claim 1, wherein the privileged mode driver includes program instructions adapted to periodically determine the operational characteristic of the physical layer hardware unit and signal the security violation.

3. The system of claim 2, wherein the processing unit includes a timer adapted to generate an interrupt signal for invoking the privileged mode driver after a predetermined interval.

4. The system of claim 2, wherein the standard mode driver includes program instructions adapted to periodically invoke the privileged mode driver.

5. The system of claim 1, wherein the privileged mode driver includes program instructions adapted to compare the control codes generated by the standard mode driver to the secure control codes and signal the security violation in response to the control codes being different than the secure control codes.

6. The system of claim 1, wherein the privileged mode driver includes program instructions adapted to query the physical layer hardware unit to determine the control codes sent by the standard mode driver, compare the control codes received by the physical layer hardware unit to the secure control codes, and signal the security violation in response to the control codes received by the physical layer hardware unit being different than the secure control codes.

7. The system of claim 1, wherein the physical layer hardware unit includes a radio configured in accordance with the assigned transmission parameters, and the privileged mode driver includes program instructions to identify an operating state of the radio, compare the operating state of the radio to the secure control codes, and signal the security violation in response to the operating state being inconsistent with the secure control codes.

8. The system of claim 7, wherein the operating state of the radio includes at least one of a transmission power level, a transmission frequency, and a transmission time slot.

9. The system of claim 1, wherein the transmission assignments include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

10. The system of claim 1, wherein the privileged mode of operation comprises a system management mode of operation.

11. The system of claim 1, wherein the standard mode driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation.

12. The system of claim 11, wherein the signal comprises a system management interrupt.

13. The system of claim 1, wherein the standard mode driver includes program instructions adapted to extract encrypted data from the digital received signal and decrypt the encrypted data to generate decrypted data including the control codes.

14. The system of claim 13, wherein the privileged mode driver includes program instructions adapted to receive the encrypted data, decrypt the decrypt the encrypted data to generate secure decrypted data, and extract the secure control codes from the decrypted data.

15. The system of claim 14, wherein the processing unit includes a memory device adapted to store the encrypted data, and the standard mode driver includes program instructions adapted to pass a pointer indicating a location of the encrypted data within the memory device to the privileged mode driver.

16. The system of claim 1, wherein the processing unit comprises a computer.

17. The system of claim 16, wherein the computer includes:

a processor complex adapted to execute the program instructions in the standard mode driver and the privileged mode driver;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware.

18. The system of claim 1, wherein the computer includes a system basic input output system (BIOS) memory adapted to store the privileged mode driver.

19. The system of claim 18, wherein the computer is adapted to load the privileged mode driver from the system BIOS into a protected memory location during initialization of the computer.

20. The system of claim 1, wherein the privileged mode driver includes program instructions adapted to prohibit further operation of the standard mode driver in response to identifying the security violation.

21. The system of claim 1, wherein the privileged mode driver includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation.

22. A method for identifying security violations in a transceiver, comprising:

receiving digital data over a communications channel in a standard processing mode of a processing unit;

extracting control codes from the digital received signal in the standard processing mode;

configuring assigned transmission parameters of a physical layer hardware unit in the transceiver in the standard processing mode based on the control codes;

transitioning the processing unit into a privileged processing mode;

extracting secure control codes from the digital received signal in the privileged processing mode;

determining an operational characteristic of the physical layer hardware unit in the transceiver in the privileged processing mode;

comparing the operational characteristic to the secure control codes in the privileged processing mode; and

signaling a security violation in response to the operational characteristic being inconsistent with the secure control codes.

23. The method of claim 22, further comprising periodically generating an interrupt signal for transitioning the processing unit into the privileged processing mode after a predetermined time interval.

24. The method of claim 22, wherein determining the operational characteristic of the physical layer hardware unit comprises determining the control codes extracted from the digital received signal in the standard processing mode.

25. The method of claim 22, wherein determining the operational characteristic of the physical layer hardware unit comprises querying the physical layer hardware unit to determine the control codes used to configure the assigned transmission parameters in the standard processing mode.

26. The method of claim 22, wherein the physical layer hardware unit includes a radio configured in accordance with the assigned transmission parameters, and determining the operational characteristic of the physical layer hardware unit comprises identifying an operating state of the radio.

27. The method of claim 26, wherein identifying the operating state of the radio comprises identifying at least one of a transmission power level, a transmission frequency, and a transmission time slot.

28. The method of claim 22, wherein transitioning the processing unit into the privileged processing mode comprises transitioning the processing unit into a system management mode of operation.

29. The method of claim 22, wherein transitioning the processing unit into the privileged processing mode comprises issuing a system management interrupt.

30. The method of claim 22, further comprising:

extracting encrypted data from the digital received signal in the standard processing mode; and

decrypting the encrypted data to generate decrypted data including the control codes.

31. The method of claim 30, further comprising:

receiving the encrypted data in the privileged processing mode;

decrypting the decrypt the encrypted data in the privileged processing mode to generate secure decrypted data; and

extracting the secure control codes from the decrypted data in the privileged processing mode.

32. The method of claim 31, wherein the processing unit includes a memory device adapted to store the encrypted data, and receiving the encrypted data further comprises providing a pointer indicating a location of the encrypted data within the memory device.

33. The method of claim 32, further comprising prohibiting further operation of the processing unit in response to identifying the security violation.

34. A modem, comprising:

means for receiving digital data over a communications channel in a standard processing mode of a processing unit;

means for extracting control codes from the digital received signal in the standard processing mode;

means for configuring assigned transmission parameters of a physical layer hardware unit in the transceiver in the standard processing mode based on the control codes;

means for transitioning the processing unit into a privileged processing mode;

means for extracting secure control codes from the digital received signal in the privileged processing mode;

means for determining an operational characteristic of the physical layer hardware unit in the transceiver in the privileged processing mode;

means for comparing the operational characteristic to the secure control codes in the privileged processing mode; and

means for signaling a security violation in response to the operational characteristic being inconsistent with the secure control codes.